JURNAL TIMES
TECHNOLOGY INFORMATICS & COMPUTER SYSTEM

Volume VII No 1, Juni 2018
*p*ISSN : 2337 – 3601
*e*ISSN : 2549 – 015X

Tersedia *online* di http://ejournal.stmik-time.ac.id

Implementasi Algoritma Transposisi Cipher Dalam Sistem Pengamanan Data Pada Jaringan LAN

Melvarina Tamba
Sekolah Tinggi Teknik Poliprofesi Medan
Jln. sei batang hari no 1,3,4 Medan
e-mail : melvarina.tam@gmail.com

Abstrak
Perancangan program pengamanan pesan menggunakan transposisi sistem kriptografi dan steganografi bertujuan untuk mengamankan substansi data rahasia apapun dengan cara menyamarkannya ke dalam media-media tertentu. Dengan cara ini keaslian data dapat dipercaya. Program ini dibuat sesuai dengan metode System Development Life Cycle (SDLC). Steganografi dengan metode Metode Cipher Transpostion yaitu mengubah urutan huruf-huruf yang ada di dalam plainteks (pesan yang belum dienkripsi) menjadi cipherteks (pesan ynag telah dienkripsi) dengan cara tertentu agar isi dari pesan tersebut tidak dimengerti kecuali oleh orang-orang tertentu. Pada cipher transposisi, huruf-huruf di dalam plainteks tetap saja, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (scrambling) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Kata kunci : Kriptographi, Chiper Transposisi Klasik, LAN

1. Latar Belakang

Masalah keamanan komputer merupakan sesuatu yang sangat penting dalam era informasi ini terutama bagi suatu organisasi atau perusahaan. Kerahasiaan data merupakan sesuatu yang sangat penting dalam keamanan data. Data pelanggan menjadi salah satu data yang sangat penting dalam kelangsungan berjalannya perusahaan. Kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Sistem yang diterapkan oleh kebanyakan instansi pada saat ini sudah kebanyakan secara terkomputerisasi, contohnya pengiriman data perusahaan, perparkiran, pembelian tiket, pembuatan identitas, dan lain sebagainya.

Tetapi pada penerapan sistem ini seiring perkembangan zaman yang terus meningkat masih banyak yang kurang efektif dan efesien dalam sistem keamanan data, sehingga memberi peluang bagi orang lain melakukan tindakan kejahatan seperti penyadapan data, penggandaan atau penduplikasian. Ketika suatu pesan ditransfer dari suatu tempat ke tempat lain, isi dari pesan tersebut dapat disadap oleh orang lain. Untuk menjaga keamanan data tersebut, maka pesan dapat di-scramble atau diubah menjadi kode yang tidak dapat dimengerti oleh orang lain. Dan mengenkripsi data-data tersebut sehingga data yang tertera merupakan sandi dari data yang asli. Metode algoritma yang digunakan untuk mengenkripsi data-data tersebut yaitu algoritma *vigenere cipher*. Dalam penelitian ini membahas tentang "Impelementasi Algoritma Transposisi Cipher Dalam Sistem Pengamanan Data Pada Jaringan LAN".

2. Landasan Teori

Sistem kriptografi terdiri dari 5 bagian yaitu [1]:

1. *Plaintext*
   Plaintext adalah pesan atau data yang bentuk aslinya. *Plaintext* merupakan masukan bagi algoritma enkripsi untuk selanjutnya digunakan istilah teks asli sebagai padanan *plaintext.*
2. *Secret Key*
   Secret key merupakan masukan bagi algoritma enkripsi yang nilainya bebas terhadap teks asli dan yang menentukan hasil keluaran algoritma enkripsi. Untuk selanjutnya digunakan istilah kunci rahasia sebagai padanan kata *secret key.*
3. *Ciphertext*
   Ciphertext adalah keluaran algoritma enkripsi. *Ciphertext* dapat dianggap sebagai pesan dalam bentuk tersembunyi. Algoritma enkripsi yang baik akan menghasilkan *ciphertext* yang terlihat acak. Untuk selanjutnya digunakan istilah sandi sebagai padanan kata *ciphertext.*
4. Algoritma Enkripsi

Algoritma enkripsi memiliki 2 masukan teks asli dan kunci rahasia. Algoritma enkripsi melakukan transformasi terhadap teks asli sehingga menghasilkan teks sandi.

5. Algoritma Dekripsi
   Algoritma dekripsi memilik 2 masukan yaitu teks sandi dan kunci rahasia. Algoritma dekripsi memulihkan kembali teks sandi menjadi teks asli bila kunci rahasia yang dipakai algoritma dekripsi sama dengan kunci rahasia yang dipakai algoritma dekripsi.

Sistem enkripsi hasus memenuhi alkaidah *correctness.* Yaitu untuk setiap $K \in K$, dengan K adalah himpunan kunci terhadap teks sandi hasil enkripsi teks asli m,c = $e_k(m)$, maka harus berlaku $d_K(c)=n$ untuk semua kenungkinan teks asli.

Berdasarkan jenis kunci yang digunakannya, algoritma kriptografi dikelompokan menjadi dua bagian, yaitu :

1. Symmetric Algorithm
   Symmetric algorithm atau disebut juga *secret key algorithm* merupakan algoritma yang kunci enkripsinya dapat dihitung dari kunci dekripsi dan begitu pula sebaliknya, kunci dekripsi dapat dihitung dari kunci enkripsi. Pada sebagian besar symmetric algorithm kunci enkripsi dan kunci dekripsi adalah sama. Symmetric algorithm memerlukan kesepakatan antara pengirim dan penerima pesan pada suatu kunci sebelum dapat berkomunikasi secara aman. Keamanan symmetric algorithm tergantung pada rahasia kunci. Pemecahan kunci berarti memungkinkan setiap orang dapat mengenkripsi dan mendekripsi pesan dengan mudah. Symmetric algorithm dapat dikelompokkan menjadi dua jenis, yaitu stream cipher dan block cipher. Stream cipher beroperasi byte per byte pada satu waktu, sedangkan block cipher beroperasi kelompok per kelompok byte yang disebut blok (block) pada satu waktu.
2. Asymmetric Algorithm
   Asymmetric algorithm atau disebut juga *public key algorithm* didesain agar memudahkan dalam distribusi kunci yang digunakan untuk enkripsi dan dekripsi. Kunci dekripsi pada public key algorithm secara praktis tidak dapat dihitung dari kunci enkripsi. Algoritma ini disebut "public key" karena kunci dapat dibuat menjadi publik. Setiap orang dapat menggunakan kunci enkripsi untuk mengenkripsi pesan, tetapi hanya orang yang memiliki kunci dekripsi yang dapat mendekripsi pesan tersebut. Pada sistem ini kunci enkripsi sering disebut kunci publik (public key), dan kunci dekripsi disebut kunci rahasia (private key).

Pada bagian ini akan didiskusikan operasi-operasi penyandian dasar untuk memberikan dasar bagi pemahaman tentang evolusi metode-metode enkripsi dan usaha-usaha cryptanalysis yang berkaitan.

Cipher Substitusi

Caesar cipher adalah cipher substitusi sederhana yang mencakup pergeseran alfabet 3 (tiga) posisi ke kanan. Caesar cipher merupakan subset dari cipher polialfabetik *Vigenere*. Pada Caesar cipher karakter-karakter pesan dan pengulangan kunci dijumlahkan bersama modulo 26. Dalam penjumlahan modulo 26, huruf-huruf A-Z dari alfabet masing-masing memberikan nilai 0 sampai 25. Tipe cipher ini dapat diserang menggunakan analisis frekuensi. Dalam analisis frekuensi, digunakan karakteristik frekuensi yang tampak dalam penggunaan huruf-huruf alfabet pada bahasa tertentu. Tipe cryptanalysis ini dimungkinkan karena Caesar cipher adalah monoalfabetik cipher/substitution cipher sederhana, dimana karakter ciphertext disubstitusi untuk setiap karakter plaintext. Serangan ini dapat diatasi dengan menggunakan substitution polialfabetik. Substitusi polialfabetik dicapai melalui penggunaan beberapa cipher substitusi. Namun substitusi ini dapat diserang dengan penemuan periode saat substitusi berulang kembali.

Cipher Transposisi

Cipher transposisi adalah salah satu jenis teknik pengenkripsian pesan dengan cara mengubah urutan huruf-huruf yang ada di dalam plainteks (pesan yang belum dienkripsi) menjadi cipherteks (pesan yang telah dienkripsi) dengan cara tertentu agar isi dari pesan tersebut tidak dimengerti kecuali oleh orang-orang tertentu.

Pada dasarnya prinsip pengubahan pesan mirip dengan anagram seperti kata "melepas" diubah menjadi "saeelpm", tapi tentu saja transposition cipher mempunyai rumus atau kunci tertentu yang diperlukan agar pesan bisa dimengerti.

Pada cipher transposisi, huruf-huruf di dalam plainteks tetap saja, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (scrambling) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakater tersebut [2].

Pada cipher ini huruf-huruf plaintext dipermutasi. Sebagai contoh, huruf-huruf plaintext A T T A C K A T D A W N dapat dipermutasi menjadi D C K A A W N A T A T T. Cipher transposisi kolumnar adalah cipher dimana plaintext ditulis secara horizontal pada kertas dan dibaca secara vertikal. Cipher transposisi dapat diserang melalui analisis frekuensi, namun cipher menyembunyikan properti statistik dari pasangan huruf-huruf.

Terdapat tiga jenis utama metode transposisi, yaitu [3]:

1. Transposisi grup

Pada metode ini, plainteks dibagi ke dalam blok-blok / grup yang ukurannya sama. Kemudian, kepada setiap blok pesan ini diaplikasikan suatu susunan karakter yang telah didefinisikan. Misalkan sebuah susunan karakter didefinisikan pada sebuah grup karakter yang panjangnya delapan, sebagai "mengumpulkan dan mengurutkan karakter bernomor prima dan diikuti sisanya". Maka hasil permutasinya (Π) ialah :

$$\Pi = c_2, c_3, c_5, c_7, c_1, c_4, c_6, c_8 \quad \text{..... (1)}$$

dengan cn adalah karakter ke-n dalam blok karakter.

2. Transposisi serial
   Metode ini mengelompokkan seluruh karakter plainteks ke dalam beberapa grup dengan aturan tertentu, kemudian cipherteks disusun dengan menyatukan grup-grup tersebut secara berurutan (serial). Misalkan sebuah plainteks P terdiri atas 20 karakter, yakni :

   $p_1p_2p_3p_4p_5p_6p_7p_8p_9p_{10}p_{11}p_{12}p_{13}p_{14}p_{15}p_{16}p_{17}p_{18}p_{19}p_{20}$

   Kemudian didefinisikan tiga grup secara berturut-turut : grup bilangan kelipatan 4 (empat), grup bilangan ganjil, dan grup sisa.

   $G1 = p_4p_8p_{12}p_{16}p_{20}$
   $G2 = p_1p_3p_5p7p_9p_{11}p_{13}p_{15}p_{17}p_{19}$
   $G3 = p_2p_6p_{10}p_{14}p_{18}$

   Maka, cipherteks C akan memiliki susunan

   $C = G_1G_2G_3$
   $= p_4p_8p_{12}p_{16}p_{20}p_1p_3p_5p_7p_9p_{11}p_{13}p_{15}p_{17}p_{19}p_2p_6p_{10}p_{14}p_{18}$

3. Transposisi kolom / baris
   Dasar dari metode ini ialah menuliskan plainteks dalam beberapa baris, kemudian cipherteks diperoleh dengan cara membacanya kolom per kolom (karakter). Berikut ialah ilustrasi dari teknik ini.

   Plainteks : INI MIRIP OPERASI TRANSPOSE PADA MATRIKS

   ditulis dalam 4 baris dan spasi dihilangkan

   INIMIRIPO
   PERASITRA
   NSPOSEPAD
   AMATRIKS

   kemudian dibaca kolom per kolom menjadi

   IPNA NESM IRPA MAOT ISSR RIEI ITPK PRAS OAD

Dari metode dasar tersebut banyak variasi yang dapat dikembangkan, salah satunya ialah melakukan pertukaran kolom dengan memanfaatkan kunci. Misalkan teknik ini akan dilakukan pada contoh sebelumnya. Karena ada sembilan kolom maka kunci yang digunakan panjangnya sembilan karakter. Misalkan kuncinya ialah TRANSPOSE, maka :

Kunci : T R A N S P O S E
Teks : I N I M I R I P O
P E R A S I T R A
N S P O S E P A D
A M A T R I K S

Pertukaran kolom dilakukan dengan cara mengurutkan karakter-karakter pada kunci menjadi:
Kunci : A E N O P R S S T
Teks : I O M I R N I P I
R A A T I E S R P

P D O P E S S A N
A T K I M R S A

3. Metode Penelitian

Algortima Sistem

Transposition cipher adalah salah satu jenis teknik pengenkripsian pesan dengan cara mengubah urutan huruf-huruf yang ada di dalam plainteks (pesan yang belum dienkripsi) menjadi cipherteks (pesan yang telah dienkripsi) dengan cara tertentu agar isi dari pesan tersebut tidak dimengerti kecuali oleh orang-orang tertentu. Pada dasarnya prinsip pengubahan pesan mirip dengan anagram seperti kata "melepas" diubah menjadi "saeelpm", tapi tentu saja transposition cipher mempunyai rumus atau kunci tertentu yang diperlukan agar pesan bisa dimengerti.

Prinsip kerja dari Metode Cipher Transposisi adalah sebagai berikut :

1. Cipher teks diperoleh dengan mengubah posisi huruf di dalam plainteks.
2. Dengan kata lain, algoritma ini melakukan transpose terhadap rangkaian huruf di dalam plainteks.
3. Nama lain untuk metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.
   Contoh : Misalkan plainteks adalah PROGRAM STUDI TEKNIK INFORMATIKA UMI dengan kunci 5.
   Untuk menentukan matrix dalam proses enkripsi digunakan rumus :

$$R = P / K \quad \text{.....(2)}$$

Keterangan :
R = Matrix Transposisi
P = Jumlah Plaintext
K = Jumlah Kunci

Enkripsi :
P = 30
K = 5
Jadi matrix transposisi dari contoh diatas berordo [6:5]
PROGRAM STUDI TEKNIK INFORMATIKA UMI

Enkripsi :
PROGRA
MSTUDI
TEKNIK
INFORM
AT IKAU
MI

Cipherteks : (baca secara vertikal)
PMTIAMRSENTIOTKFIGUNOKRDIRAAIKMU

Dekripsi : Bagi panjang cipherteks dengan kunci. (Pada contoh ini 30 / 6 = 5)
PMTKRK
RSEIMIA
OTKNAU
GUNFTM
RDIOII
AI

Plainteks: (baca secara vertikal)
PROGRAM STUDI TEKNIK INFORMATIKA UMI

Transposition ciphers mengatur ulang huruf-huruf dari plaintext tanpa menggantinya. Sebagai contoh, transposition cipher yang sangat sederhana adalah therail fence, di mana plaintext ditulis per huruf dalam dua baris dan kemudian dibaca per baris untuk dijadikan ciphertext.

Misalkan plainteksnya adalah "TOLONG PERMUTASIKAN PESAN INI YA", maka langkah pertama ialah mengelompokkan plainteks itu ke dalam blok-blok yang panjangnya delapan karakter, yaitu seperti berikut ini:

TOLONG P
ERMUTASI
KAN PESA
N INI YA
(Catatan : spasi diperhitungkan)

Langkah berikutnya, aturan permutasi yang telah ada diterapkan ke masing-masing blok pesan, yaitu menjadi:

OLN TOGP
RMTSEUAI
ANPSK EA
IIYNN A

Terakhir, blok-blok pesan itu disatukan kembali menjadi cipherteks yang utuh, seperti :

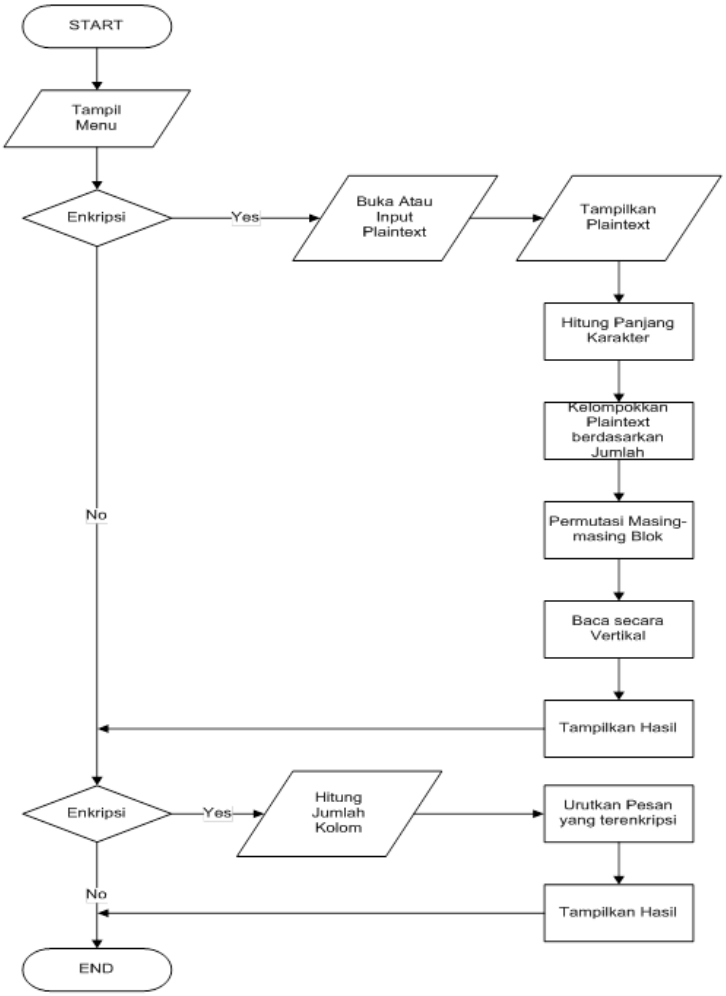
OLN TOGPRMTSEUAIANPSK EA IIYNNA

Bila jumlah karakter dalam plainteks bukan kelipatan dari panjang Π, maka pada akhir pesan dapat ditambahkan (padding), karakter-karakter dummy. Selain itu, terdapat alternative lain dalam metode ini, diantaranya dengan membuang spasi.

Untuk memperoleh plainteks kembali, penerima pesan harus mencari jumlah kolom dengan membagi panjang pesan dengan panjang kunci. Kemudian dia akan dapat menulis kembali pesan dalam kolom-kolom. Selanjutnya mengurutkan kembali kolom tersebut dengan melihat kata kunci.

Flowchart

Sistem Pengamanan Data Text Menggunakan Kriptografi dengan Metode Cipher Transposisi seperti dapat dilihat pada gambar 1 berikut :

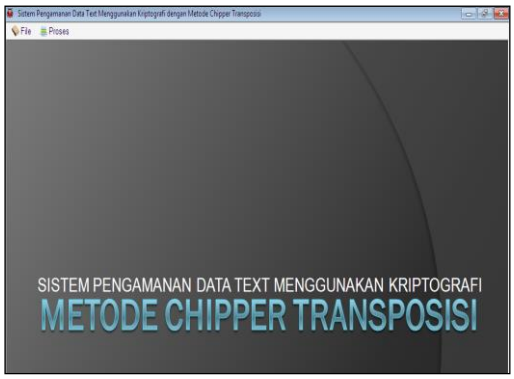


Gambar 1. Diagram Metode Chipper Transposisi

4. Hasil Penelitian

Form Menu Utama

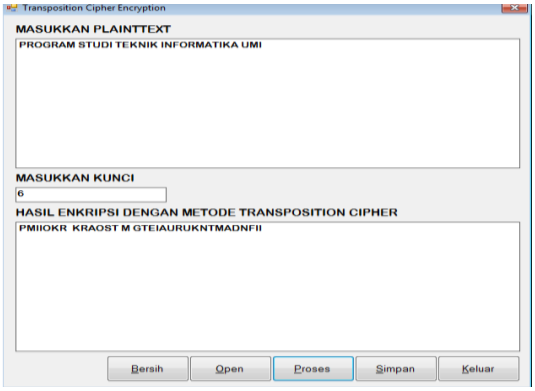
Form menu utama merupakan form untuk menampilkan menu-menu yang dapat digunakan oleh user. Tampilan form menu utama dapat dilihat pada gambar di bawah ini:



Gambar 2. Form Menu Utama

Form Enkripsi

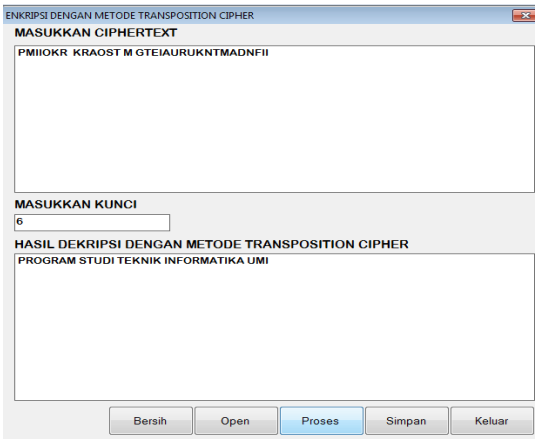
Form enkripsi merupakan form untuk melakukan proses enkripsi. Proses enkripsi data pegawai dilakukan pada saat menekan tombol simpan. Data yang disimpan merupakan data yang sudah dienkripsi. Bentuk tampilan form enkripsi dapat dilihat pada gambar dibawah ini:



Gambar 3. Tampilan Form Enkripsi

Form Dekripsi

Form dekripsi merupakan form untuk melakukan proses dekripsi. Proses dekripsi teks dilakukan pada saat menekan tombol. Bentuk rancangan form dekripsi dapat dilihat pada gambar dibawah ini.



Gambar 4. Tampilan Form Dekripsi

Metode cipher subtitusi dilakukan dengan menggeser bit sebanyak yang user inginkan. Contohnya seperti screenshoot diatas dimasukkan "PROGRAM STUDI TEKNIK INFORMATIKA UMI". Metode ini sangat mengandalkan ASCII, perubahan yang dilakukan pasti seragam.

Semua string yang dimasukkan di konversi menjadi char, masing-masing karakter memiliki *address matrix* satu dimensi. Selanjutnya seluruh karakter akan dihitung panjang string atau banyaknya karakter. String diatas memiliki panjang 30 karena terdapat nilai konstan = 5, untuk membagi karakter kedalam sebuah matrix kelipatan 5, maka panjang karakter harus habis dibagi 5. Jika memiliki sisa hasil bagi (modulus), maka dibelakang string ditambahkan karakter " " sebanyak jumlah modulus.

Setelah itu dari total seluruhnya ada 30 karakter, maka akan dimasukkan kedalam matrix 6 x 5. Bilangan 6 didapat dari perhitungan pembagian 30/5=6. Karakter akan dimasukkan mulai dari kanan bawah ke kiri bawah, kanan tengah ke kiri tengah dan seterusnya.

Enkrip transposisi akan segera dilakukan, sistem akan mulai mengidentifikasi karakter secara berurutan. Misalnya 6 karakter pertama akan ditempatkan secara fertical. Selanjutnya, karakter yang telah disusun secara vertical akan dibaca secara horizontal. Pembacaan secara horizontal tersebut merupakan hasil enkripsinya.

Untuk mengembalikannya diperlukan proses dekripsi, yang dimasukkan haruslah ciphertext. Ketika ciphertext dimasukkan kedalam sebuah sistem *decode* dari sebuah kriptografi transposition cipher mulailah proses pemulihan. Pemeriksaan dilakukan mulai dari panjang string. Jika kurang dari konstan 6, maka ditambahkan spasi sebanyak jumlah modulus, cara yang sama ketika memulai system *encode*, setelah melakukan konversi dari string ke char dilakukan penempatan karakter ke dalam matrix 6 x 5.

5. Kesimpulan

Beberapa kesimpulan yang dapat diambil dari penelitian yang telah dilakukan diatas diantaranya :

1. Variasi dari algoritma transposisi sangat banyak dan terapannya dapat bermacam-macam.
2. Algoritma transposisi cipher mempunyai beberapa kekuatan dan juga kelemahan. Algoritma ini akan lebih kuat lagi apabila pada akhir proses enkripsi cipherteks di-XOR-kan dengan kata kunci, sehingga penebakan terhadap kunci sulit untuk dilakukan.
3. Algoritma transposisi jika diterapkan secara stand alone, akan terdapat celah untuk mendapatkan kunci enkripsi dan dekripsi.
4. Tiap proses penukaran dan transposisi membutuhkan cost waktu yang cukup besar.
5. Algoritma pencarian kunci pada algoritma diatas terkadang dapat menghasilkan nilai yang sama pada beberapa kasus. Namun peluang terjadinya hal ini sangat kecil sekali.
6. Algoritma kriptografi Metode Cipher Transposisi dapat diterapkan pada pengamanan password untuk menjaga keamanan data.
7. Belum ada teknik pembobolan lain yang lebih efektif daripada brute force attack. Jadi untuk ukuran kunci sistem penyandian dengan Metode Transposisi Cipher masih tergolong bagus.

6. Daftar Pustaka

[1] R. Sadikin, Kriptografi untuk keamanan jaringan dan implementasinya dalam bahasa Java, Yogyakarta: Andi, 2012.

[2] D. S. Nasution, "Penerapan Metode Linear Kongruen dan Algoritma Vigenere Cipher Pada Aplikasi Sistem Ujian Berbasis LAN," *Jurnal Pelita Informatika Budi Darma,* vol. IV, no. 1, pp. 1-10, 2013.

[3] A. Boyke, "Rancangan Dan Analisis Cipher Berbasis Algoritma Transposisi Dengan Periodisasi Kunci," Institut Teknologi Bandung, Bandung, 2010.